

Solving the Tensor Isomorphism Problem for special orbits with low rank points: Cryptanalysis and repair of an Asiacrypt 2023 commitment scheme

Valerie Gilchrist¹, Laurane Marco², Christophe Petit^{1,3}, Gang Tang⁴

¹ Université Libre de Bruxelles, Brussels, Belgium

² EPFL, Lausanne, Switzerland

³ University of Birmingham, Birmingham, United Kingdom

⁴ University of Technology Sydney, NSW, Australia

Abstract. The Tensor Isomorphism Problem (TIP) has been shown to be equivalent to the matrix code equivalence problem, making it an interesting candidate on which to build post-quantum cryptographic primitives. These hard problems have already been used in protocol development. One of these, MEDS, is currently in Round 1 of NIST’s call for additional post-quantum digital signatures.

In this work, we consider the TIP for a special class of tensors. The hardness of the decisional version of this problem is the foundation of a commitment scheme proposed by D’Alconzo, Flamini, and Gangemi (Asiacrypt 2023). We present polynomial-time algorithms for the decisional and computational versions of TIP for special orbits, which implies that the commitment scheme is not secure. The key observations of these algorithms are that these special tensors contain some low-rank points, and their stabilizer groups are not trivial.

With these new developments in the security of TIP in mind, we give a new commitment scheme based on the general TIP that is non-interactive, post-quantum, and statistically binding, making no new assumptions. Such a commitment scheme does not currently exist in the literature.

1 Introduction

Group actions have proven very useful in the transition to post-quantum cryptography. They provide a quantum-safe algebraic operation in certain instantiations, making it easy to use them as a replacement in previously classical schemes. Recently, isogenies have been the most well-studied example of a post-quantum group action. We can find, however, group actions from other hard problems, some of which have already been proposed for use in post-quantum cryptography. Such group actions include alternating trilinear forms [42], lattices [18], polynomials [35], linear codes [5, 13], and tensors [28].

* Authors listed in alphabetical order: see <https://www.ams.org/profession/leaders/CultureStatement04.pdf>. This work was funded in part by a FRIA grant by the National Fund for Scientific Research (F.N.R.S.) of Belgium. Date of this document: 2024-02-26.

The work of [24] shows that three of these hard problems, the matrix code equivalence problem, the trilinear form equivalence problem, and the tensor isomorphism problem (TIP) are all equivalent. Particularly given a 3-tensor with dimensions l, m, n , we can naturally represent it as a $[l \times m, n]$ -matrix code. Thus, though our focus in this work will be on TIP, we will be inherently studying the security of all three of these problems. Two recent independent works [13,28] proposed using tensor isomorphism (or matrix code equivalence) for cryptographic purposes from the different algebraic structures of tensors and codes. Very recently, a digital signature scheme, MEDS [12], based on matrix code equivalence was submitted to the NIST standardization competition for post-quantum signatures as a round 1 candidate. The security of MEDS, that is, the algorithm of matrix code equivalence, has been studied in several works [12,13,15,38]. We proceed to briefly review the state-of-the-art algorithms for matrix code equivalence, and hence TIP.

Algorithms solving matrix code equivalence. There are three types of algorithms for matrix code equivalence. The first one uses algebraic methods, whereby matrix code equivalence is translated into solving systems of polynomial equations. Gröbner basis techniques are often employed for this approach, albeit with efficiency contingent upon the values of l, m and n . Notably, efficiency diminishes significantly when these dimensions become slightly large. The second is the graph-theoretic algorithm [38], which involves transforming matrix codes into quadratic mappings, thereby facilitating the adaptation of algorithms designed for Quadratic Maps Linear Equivalence (QMLE) [8]. Nevertheless, this approach does not perform well when $l = m = n$. The last one is the Leon-like algorithm, which is an adaptation of the code equivalence problem algorithm on the Hamming metric. The basic idea comes from the observation that equivalence preserves the Hamming weight as well as the weight distribution of the codewords. Leon’s [30] algorithm entails finding the set of codewords with minimal Hamming weight in two given codes, which can reveal enough information to recover the equivalence. Beullens [7] recently improved this algorithm by building two lists of codewords with a particular weight and then searching for collisions between them to recover the equivalence. This approach naturally translated to matrix code [13]: by creating two lists of matrices with low rank in the two given matrix codes one can then find the collision to recover the equivalence.

In this work, we will consider TIP, but on special orbits. This problem was first introduced at ASIACRYPT 2023 by D’Alconzo, Flamini and Gangemi [17] in the context of a commitment scheme construction. While the general TIP considers tensors that are generated randomly, which we call *random tensors*, the work of [17] restricts to the use of very particular tensors with a lot of structure, or *structured tensors*. Their commitment scheme uses the orbits of two of these structured tensors, which they conjecture is still secure.

1.1 Our contributions

In this paper, we propose polynomial-time algorithms for the decisional and computational versions of TIP on special orbits. This implies the commitment scheme proposed by D’Alconzo, Flamini and Gangemi in Asiacrypt 2023 is broken. We also propose a countermeasure to fix the commitment scheme. We summarize our contributions in what follows.

Algorithms for tensor isomorphism on special orbits. We present a polynomial-time algorithm for the TIP on special orbits. One observation is that some low-rank points exist for the tensors on these special orbits. This allows us to distinguish tensors on two different orbits, which implies that the decisional TIP is broken. Another observation is that the automorphism groups of these structured tensors are not trivial, that is, they have stabilizers. Therefore, we can avoid finding collisions and quickly recover an equivalent isomorphism which solves the computational TIP.

Regarding the commitment scheme proposed by D’Alconzo, Flamini and Gangemi, its security is based on the hardness of decisional TIP on these structured tensors. We implement our algorithms and use them to break the hiding property of the scheme, as well as recover the random values used when creating the commitment. These algorithms render the scheme completely insecure; see more details in Section 3.

Repairing Asiacrypt 2023 scheme. We provide a countermeasure to repair the commitment scheme from [17] using *random* (instead of structured) tensors. Our new scheme fills the gap of a post-quantum, non-interactive commitment scheme from non-transitive group actions, which was the aim of the Asiacrypt 2023 commitment scheme [17], and which is still missing in the literature. We stress that our new scheme makes no new assumptions, but only depends on already existing hard problems from random tensors. The scheme we propose is statistically binding and computationally hiding. We conclude by proposing a zero-knowledge proof of opening for our new commitment scheme.

Organization. In Section 2 we summarize the relevant concepts pertaining to group actions, tensors, commitment schemes, and the protocol we will be attacking from [17]. In Sections 3.1 and 3.2 we discuss low rank points and our attack on the hiding property of [17], and in Sections 3.3, 3.4, and 3.5, we compute stabilizers and give an attack that recovers the full secret. Finally, in Section 4, we give a repair on their commitment scheme that preserves the non-interactive structure and still has statistical binding, with a discussion on relevant zero-knowledge proofs in Section 4.1.

2 Preliminaries

In the rest of this work, we denote by $\mathbf{1}_A(x)$ the function taking value 1 if $x \in A$ and 0 otherwise. We write PPT to stand for Probabilistic Polynomial Time. We

call a function *negligible*, written $\text{negl}(\lambda)$, if its absolute value is asymptotically dominated by $O(x^{-n})$ for all $n > 0$.

2.1 Cryptographic group actions

Group actions have been of interest in cryptography because they sometimes provide an easy way to transition classical cryptosystems to post-quantum ones. The first well-studied instance of a group action used in cryptography was in works from Couveignes [14], and Rostovstev and Stolbunov [39], where they developed a Diffie-Hellman-like key exchange scheme from the isogeny group action.

The seminal work from Alamiati, De Feo, Montgomery, and Patranabis in [1] generalizes the hard problems taken from the isogeny group action for use with any group action. In doing so, they establish standard definitions and notation that have since been upheld in the field, providing a valuable common ground for proceeding works. To begin, we recall some of these definitions that will be relevant to our work.

Definition 1 (Group action). *We say that a group G acts on a set X if there exists a map $\star : G \times X \rightarrow X$ such that :*

- *Identity:* If e is the identity element of G , then for any $x \in X$, $e \star x = x$;
- *Compatibility:* For any $g, h \in G$, and any $x \in X$, $(gh) \star x = g \star (h \star x)$.

Such a group action can be denoted (G, X, \star) .

We call a group action *transitive* if for any two elements $x, y \in X$, there exists a group element $g \in G$ mapping x to y , i.e. $y = g \star x$. We say a group action is *free* if for each $g \in G$ it is the identity element if and only if there exists an element $x \in X$ such that $x = g \star x$. A group action is called *regular* if it is both transitive and free.

Definition 2 (Orbit). *The orbit, O_x , of an element $x \in X$, is all the $y \in X$ for which there exists an element mapping x to y i.e. $O_x = \{y \in X \mid \exists g \in G, y = g \star x\}$.*

We can reformulate transitivity in terms of orbits : an action is transitive if for all $x, y \in X$, we get that $O_x = O_y$.

Since we are considering group actions in the context of cryptography, we will only be concerned with *effective group actions*.

Definition 3 (Effective group action (EGA)). *We call a group action $\star : G \times X \rightarrow X$ effective if the following properties hold :*

- *G is finite and there exists a PPT algorithm for the following operations : group operation, computation of inverses, membership testing, equality testing and sampling.*
- *X is finite and there exists a PPT algorithm for membership testing and for computing a unique representation of elements in X .*

- There exists a distinguished element $x_0 \in X$ such that its bit-string representation is known. We call this point the origin.
- \star can be computed efficiently for any $g \in G, x \in X$.

When creating cryptography from group actions, we will want to be able to actually evaluate the group action, hence we will limit ourselves to EGAs. In some instances where only a portion of the group or set can be evaluated efficiently, we can restrict to such a subset. This is called a *Restricted Effective Group Action (REGA)*.

We can impose some additional properties to be fulfilled by the group action in order to build specific cryptographic constructions. We recall a definition from [17] that will be useful later on in this work.

Definition 4 (Decisional Group Action Inverse Problem). *Let (G, X, \star) be a group action, and $t_0, t_1 \in X$ lie in distinct orbits. The decisional Group Action Inverse Problem (dGA-IP) game for (G, X, \star) is described in Figure 1. For an adversary \mathcal{A} against the dGA-IP game, we define the advantage Adv as follows :*

$$\text{Adv}(\mathcal{A}) = \Pr[\text{dGA-IP}(\mathcal{A}) \rightarrow 1] - \frac{1}{2}.$$

```

dGA-IP( $\mathcal{A}$ )
1:  $c, b \xleftarrow{\$} \{0, 1\}$ 
2:  $g, g' \xleftarrow{\$} G$ 
3:  $s \leftarrow g \star t_c$ 
4: if  $b = 1$  then
5:    $t \leftarrow g' \star s$ 
6: end if
7: if  $b = 0$  then
8:    $t \leftarrow g' \star t_{1-c}$ 
9: end if
10:  $\mathcal{A}(s, t) \rightarrow b'$ 
11: return  $b' = b$ 

```

Fig. 1. The dGA-IP game

2.2 Tensors over finite fields

We recall some results on tensors, following the notation introduced in [17].

Fix a finite field \mathbb{F}_q for a prime q , and ℓ, m, n positive integers. Then given bases $\{e_i\}_{i=1}^\ell, \{f_i\}_{i=1}^m, \{g_i\}_{i=1}^n$ of $\mathbb{F}_q^\ell, \mathbb{F}_q^m, \mathbb{F}_q^n$, respectively, a 3-tensor $v \in \mathbb{F}_q^\ell \otimes \mathbb{F}_q^m \otimes \mathbb{F}_q^n$ is defined as follows

$$v = \sum_{i=1}^{\ell} \sum_{j=1}^m \sum_{k=1}^n v(i, j, k) e_i \otimes f_j \otimes g_k.$$

Alternatively a 3-tensor, v , can be represented as a 3-way array of field elements

$$v = [[v(i, j, k)]]_{i,j,k=1}^{l,m,n} \in \mathbb{F}_q^{l \times m \times n}.$$

Note, in the same way matrices encode bilinear forms, 3-tensors encode trilinear forms. More precisely, given a 3-tensor v , one can associate the 3-linear form $m : \mathbb{F}_q^l \times \mathbb{F}_q^m \times \mathbb{F}_q^n \rightarrow \mathbb{F}_q$ defined as

$$m(x^1, x^2, x^3) = \sum_{i_1=1}^l \sum_{i_2=1}^m \sum_{i_3=1}^n v(i_1, i_2, i_3) x_{i_1}^1 x_{i_2}^2 x_{i_3}^3.$$

For the rest of this work, we restrict to the case where $l = m = n$. We will also only be concerned with 3-tensors, even if not explicitly stated, since the work from [24] gives an equivalence between isomorphism problems on 3-tensors and higher dimensional d -tensors. This makes our study of 3-tensors an optimal instance of these problems. Let \mathbf{V} be the tensor space $\mathbf{V} = \mathbb{F}_q^n \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^n$, and we will use the canonical basis $\{e_i\}_{i=1}^n$ on \mathbb{F}_q^n to construct tensors.

Tensor rank. An essential invariant of tensors that we will be considering carefully is their *rank*.

Definition 5 (Rank 1 tensor). A tensor, $v \in \mathbf{V}$, is said to have rank 1 if it can be written as $v = a \otimes b \otimes c$, for $a, b, c \in \mathbb{F}_q^n$.

Definition 6 (Rank of a tensor). The rank of a tensor, $v \in \mathbf{V}$, is the minimal r such that we can write v in the form $v = \sum_{i=1}^r w_i$, where $\{w_i\}_{i=1}^r \subset \mathbf{V}$ is a set of rank 1 tensors.

Problem 1 (Computational Tensor Rank Problem). Given a tensor $v \in \mathbf{V}$, compute $\text{rank}(v)$.

It has been shown that Problem 1 is NP-hard [25, 26, 40]. In [25] it is also proven to be NP-complete over finite fields.

It is shown in [26] that other tensor related problems are NP-hard. These include the decisional and computational versions of problems investigating eigenvalues, singular values, and spectral norms of tensors. These problems, however, are beyond the scope of this paper.

Group action on tensors. We can further obtain hard problems from tensors by defining a group action on them.

More concretely, the tensors are being acted on by the group $G = \text{GL}(n, q) \times \text{GL}(n, q) \times \text{GL}(n, q)$, where $\text{GL}(n, q)$ denotes the general linear group of degree n over \mathbb{F}_q , in the following way:

$$\begin{aligned} \star : G \times \mathbf{V} &\rightarrow \mathbf{V}, \\ \left((A, B, C), \sum_{i,j,k} v(i, j, k) e_i \otimes e_j \otimes e_k \right) &\mapsto \sum_{i,j,k} v(i, j, k) A e_i \otimes B e_j \otimes C e_k, \end{aligned} \quad (1)$$

for $v(i, j, k) \in \mathbb{F}_q$.

Lemma 1. *Let $(A, B, C) \in G$, and $v \in \mathbf{V}$. Then $\text{rank}((A, B, C) \star v) = \text{rank}(v)$. In other words, (\star) preserves rank.*

Proof. We can decompose $(A, B, C) \star v$ into a sum as shown in Equation 1, giving us an upper bound on its rank.

To lower bound the rank we first notice that A, B, C are all invertible matrices, thus they have full rank. Therefore $\{Ae_i\}_{i=1}^n \otimes \{Be_i\}_{i=1}^n \otimes \{Ce_i\}_{i=1}^n$ is still a basis for \mathbf{V} , meaning we will not get any new linear dependencies. \square

Given this group action on tensors, we can consider two additional potentially hard problems.

Problem 2 (Decisional Tensor Isomorphism Problem). Given two tensors $v_0, v_1 \in \mathbf{V}$, decide whether there exists $(A, B, C) \in G$ such that $(A, B, C) \star v_0 = v_1$.

Problem 3 (Computational Tensor Isomorphism Problem). Given two tensors $v_0, v_1 \in \mathbf{V}$, such that $(A, B, C) \star v_0 = v_1$ for some $(A, B, C) \in G$, compute (A, B, C) .

We can rephrase these problems in terms of *orbits*, from Definition 2 : Problem 2 asks to determine whether two tensors belong to the same orbit; Problem 3 asks to determine the isomorphism mapping two elements from the same orbit.

2.3 Commitment schemes

Commitment schemes have many real-world use cases, finding applications in multiparty computations, zero-knowledge proofs, and coin tossing [21, 29, 31, 34, 37].

A commitment scheme is used when a sender wants to commit to some value, m , without initially revealing it to the receiver. Instead, the sender will commit to m by computing a commitment, c , that depends on m , and send it to the receiver. At a later time, the sender will reveal m , and the receiver should be able to verify that c was computed using b . The key properties here are *hiding*, which means c should reveal nothing about m ; and *binding*, which means no other value $m' \neq m$ should be able to open c . We proceed to give formal definitions for a commitment scheme and its security properties.

Definition 7 (Commitment scheme). *A commitment scheme is defined by a message space, \mathcal{M} , randomness space, \mathcal{R} , a commitment space, \mathcal{C} , and a tuple of algorithms, $(\text{Setup}, \text{Commit}, \text{Verify})$, defined in the following way :*

- $\text{Setup}(1^\lambda) \rightarrow \text{pp}$: *This PPT algorithm takes as input a security parameter λ in unitary form and returns some public parameters pp which will be implicitly given as inputs to the proceeding two algorithms.*
- $\text{Commit}(m, r) \rightarrow c$: *This PPT algorithm takes as input a message $m \in \mathcal{M}$ and randomness $r \in \mathcal{R}$ and outputs a commitment value $c \in \mathcal{C}$.*
- $\text{Verify}(c, (m, r)) \rightarrow 0/1$: *This is a deterministic algorithm which, given as input $c \in \mathcal{C}$, $(m, r) \in \mathcal{M} \times \mathcal{R}$ returns 1 if $\text{Commit}(m, r) = c$ and 0 otherwise.*

In the case of a *bit commitment scheme*, the committed messages are restricted to two possible values, 0 or 1.

Definition 8 (Hiding Security). A commitment scheme (Setup, Commit, Verify) is hiding if for any PPT adversary, \mathcal{A} , the advantage, Adv , is negligible, where Adv is defined as

$$\text{Adv} = \Pr[\text{Hiding}(\mathcal{A}) \rightarrow 1]$$

and the Hiding game is defined in Figure 2.

Hiding(\mathcal{A})
 1: $\text{Setup}(1^\lambda) \rightarrow \text{pp}$
 2: $\mathcal{A}(\text{pp}) \rightarrow m_0, m_1, st$
 3: $b \xleftarrow{\$} \{0, 1\}, r \xleftarrow{\$} \mathcal{R}$
 4: $c \leftarrow \text{Commit}(m_b, r)$
 5: $\mathcal{A}(c, st) \rightarrow b'$
 6: **return** $b' = b$

Fig. 2. The Hiding game

Remark 1. Note that in the case of a bit commitment scheme, we have $\mathcal{M} = \{0, 1\}$, and in the Hiding game the adversary does not choose m_0, m_1 , rather the bit committed is the one sampled by the game, i.e. one can remove Line 2 in Figure 2 and set $m_b = b$.

Definition 9 (Binding Security). A commitment scheme (Setup, Commit, Verify) is binding if for any adversary \mathcal{A} the advantage Adv is either zero or negligible, where Adv is defined as

$$\text{Adv} = \Pr[\text{Binding}(\mathcal{A}) \rightarrow 1]$$

and the Binding game is as defined in Figure 3.

Binding(\mathcal{A})
 1: $\text{Setup}(1^\lambda) \rightarrow \text{pp}$
 2: $\mathcal{A}(\text{pp}) \rightarrow m_0, m_1, r_0, r_1$
 3: **return** $(m_0 \neq m_1) \wedge \text{Commit}(m_0; r_0) = \text{Commit}(m_1; r_1)$

Fig. 3. The Binding game

When \mathcal{A} has unbounded complexity and $\text{Adv} = 0$, it is called *perfectly* binding. When \mathcal{A} has unbounded complexity and $\text{Adv} = \text{negl}(\lambda)$, it is called *statistically* binding. When Adv is PPT, and $\text{Adv} = \text{negl}(\lambda)$ it is called *computationally* binding.

2.4 Asiacrypt 2023’s commitment scheme from tensors

While there is already literature about commitment schemes [33, 36], developing post-quantum equivalents is necessary in order to curb the risk of future quantum attacks. Many post-quantum commitments exist from lattice-based assumptions with recent constructions such as [2, 6, 19], code-based assumptions [27, 32], isogeny-based assumptions [41] and *transitive* group actions [9, 11, 28]. In [17], at Asiacrypt 2023, D’Alconzo, Flamini, and Gangemi describe a general bit commitment framework from post-quantum *non-transitive* group actions that they call GACE (Group Action with Canonical Element), and then give an example instance using tensors in Section 6.2 of their work.

In particular, they take inspiration from the fact that it is widely believed to be hard to compute the rank of a random tensor (see Section 2.2), and proven NP-hard [25, 26, 40]. In the paper they provide a method of constructing a distinguished element for any rank, such that given the rank it is easy to verify the correctness of the original claim. Let $b \in \{0, \dots, n-1\}$, then their distinguished element is

$$t_b := \sum_{i=1}^{n-b} e_i \otimes e_i \otimes e_i. \quad (2)$$

In their commitment scheme they use t_b to create either an n -rank tensor or an $(n-1)$ -rank tensor, thereby encoding a bit $b \in \{0, 1\}$. They then sample an element $(A, B, C) \in G = \text{GL}(n, q) \times \text{GL}(n, q) \times \text{GL}(n, q)$, and compute the commitment $c = (A, B, C) \star t_b$ via the group action described in Equation 1. The sender sends the commitment c to the receiver. When the sender is ready, they will reveal $(A, B, C), b$. The receiver can then easily check that $c = (A, B, C) \star t_b$, and so has rank $n - b$.

Parameters. There are no parameters given for the commitment scheme from [17]. Though our attacks run in polynomial time complexity, we would like a concrete example instance of the commitment scheme on which to test the algorithms outlined in Section 3. In particular, we will consider the parameters outlined in MEDS [12], a post-quantum signature from matrix code equivalences, submitted to the NIST competition for post-quantum signatures. Their proposed choices of vector dimension and field size, (n, q) , are $(14, 4093)$, $(22, 4093)$, $(30, 2039)$.

The matrix code equivalence problem is polynomial equivalent to the general trilinear form equivalence problem and the tensor isomorphism problem as noted in [24], meaning parameter sizes should be the same across all of these hard problems. Though, [17] does not rely on a pure form of the tensor isomorphism problem.

2.5 The MinRank problem

In Section 3 we will be exploring how low rank points can affect the security of some tensor-based hard problems. For this, we will need a way of solving a MinRank instance. Here we summarize the relevant results from [4], the current

state-of-the-art for this problem. The authors of this work revise the algebraic approach to MinRank, and thus completely avoid the use of a Gröbner basis computation for some parameters, keeping all the equations linear. When applying this approach to three NIST candidate key exchange schemes, they were able to improve upon or match the state-of-the-art attacks.

The MinRank problem is as follows:

Problem 4 (MinRank problem). Given an integer $r \in \mathbb{N}$, and k matrices $M_1, \dots, M_k \in \mathbb{F}_q^{m \times n}$, determine field elements x_1, \dots, x_k not all zero, such that

$$\text{rank}\left(\sum_{i=1}^k x_i M_i\right) \leq r.$$

In previous works [3], the MinRank problem was solved by creating equations using *coefficient* variables and *support* variables depending on maximal minor equations. This system of equations would then be solved using a Gröbner basis algorithm. In [4], they instead define even more linear equations using the coefficient and support variables. So many, in fact, that they are sufficient for solving the entire problem, thereby avoiding the Gröbner basis computation in many cases.

The algorithm. We are given n matrices, M_1, \dots, M_n , of size $n \times n$, and a target rank r . We want to find $\{x_i\}_{i=1}^n$ such that $\mathbf{M} := \sum x_i M_i$ has rank r . So the entries of \mathbf{M} are linear expressions in the variables x_i . When \mathbf{M} has rank r , we can write it as $\mathbf{M} = SR$, where columns of the $n \times r$ matrix S form a basis for the column-space of \mathbf{M} , and the $r \times n$ matrix R contains a basis for the row-space of \mathbf{M} . The entries in S and R are referred to as the *support* and *coefficient* variables, respectively. The matrix R will necessarily have full rank r . Hence, if we add a row from \mathbf{M} to it, all of its maximal minors will be vanishing. These vanishing maximal minors give us algebraic equations depending on the x_i and the entries of R . We can do this for each row of \mathbf{M} , obtaining enough equations to linearize and solve for the x_i .

2.6 Sigma protocols

We give below the definition of a sigma protocol that will be of use in Section 4.1.

Definition 10 (Sigma protocol). *Given a language $L \in NP$ over an alphabet Z defined by a relation R , a sigma protocol for L is a pair of interactive machines $\mathcal{P}(x, w)$ and $\mathcal{V}(x)$ such that*

- \mathcal{V} is polynomially bounded.
- \mathcal{P} starts with a message, a , \mathcal{V} answers with a challenge, $e \in_U E$, \mathcal{P} terminates with a response, z . \mathcal{V} accepts (returns 1) or rejects (returns 0) only depending on (x, a, e, z) .

- *Special soundness*: there exists a polynomially bounded algorithm \mathcal{E} called extractor such that for any x , if $(x, a, z; r)$ and $(x, a, z; r')$ are two accepting views for \mathcal{V} such that $e \neq e'$ where $e = \mathcal{V}(x, a; r)$ and $e' = \mathcal{V}(x, a; r')$, then $\mathcal{E}(x, a, e, z, e', z')$ yields w such that $R(x, w)$.
- *Special honest-verifier zero-knowledge* : there exists a polynomially bounded algorithm Sim called simulator such that for any $x \in L$ and e , the transcript (a, e, z) of the interaction $\mathcal{P} \xleftrightarrow{x} \mathcal{V}(r_V)$ conditioned to e has the same distribution as $\text{Sim}(x, e; r)$.

We call x the statement and w the witness.

A sigma-protocol can be turned into a non-interactive zero-knowledge proof using the Fiat-Shamir transform [20].

3 Solving Tensor Isomorphism Problems in t_b orbits

In this section we focus on attacking the commitment scheme from [17], which uses special cases of tensor hard problems. We begin in Section 3.1 by establishing some background on the rank of points in tensors. This will help us in Section 3.2, where we focus on attacking a variant of the Decisional Tensor Isomorphism Problem (DTI, see Problem 2) present in their commitment scheme, and provide a polynomial time attack on it. We then explore some elements of the stabilizer group of the family of tensors $\{t_b : b \in \mathbb{Z}_n\}$ in Section 3.3. Lastly, in Sections 3.4 and 3.5, we use these findings to attack their variant of the Computational Tensor Isomorphism Problem (CTI, see Problem 3).

All the algorithms and experiments described in the proceeding sections were coded in Magma, and can be found at

<https://anonymous.4open.science/r/tensor-group-action-CB25/> .

3.1 Computing the rank of points

In the case of tensors, we can first choose to view a 3-tensor, $g \in \mathbf{V}$, as a list of n matrices $G_1, \dots, G_n \in \mathbb{F}_q^{n \times n}$. Then we can define the rank of a point in that tensor.

Definition 11 (Rank of a point). *Let $g \in \mathbf{V}$ be a tensor, written in the form $g = [G_1, \dots, G_n]$. Then the rank of the point $u := [u_1, \dots, u_n] \in \mathbb{F}_q^n$ in g is exactly the matrix rank of $u_1 G_1 + \dots + u_n G_n$.*

We denote this value as $\text{rank}_q(u)$.

Computing the rank of points in a tensor will be useful to us later on. In the rest of this paper, when talking about the rank of points, we will consider points up to scalar multiplication, unless stated otherwise.

Lemma 2. *Let $v \in \mathbf{V}$ be a tensor. Denote $L_k(v) := \{u \in \mathbb{F}_q^n : \text{rank}_v(u) = k\}$ to be the set of rank k points in v . Now let $(A, B, C) \in G$ be an isomorphism, and $w = (A, B, C) \star v$. Then $|L_k(v)| = |L_k(w)|$.*

Proof. This follows directly from the fact that tensor rank is preserved under isomorphism (see Lemma 1) together with the Rank-Nullity Theorem. \square

When considering tensors, Lemma 2 tells us that points of fixed rank in a tensor are preserved via the group action (\star) from Equation 1. Computing a group action in this case amounts to transforming the bases of \mathbb{F}_q^n being used to compute the tensor, to new bases, via linear transformations (recall we require three bases of \mathbb{F}_q^n). Hence, the overall structure or rank of the tensor does not change.

Rank 0 points in tensors, when considering a tensor as a list of matrices, means that there exists some linear dependency between these matrices. So transforming the bases of \mathbb{F}_q^n preserves this dependency, regardless of the exact changes of bases being used. Solving for these points can be done with Gaussian elimination, as we will see in Section 3.2. Solving for any higher rank points requires more care because they do not have any linear dependencies. To do these computations we will have to resort to solving the MinRank Problem, described in Section 2.5.

3.2 Hiding attack

We now describe an attack that breaks the hiding property of the commitment scheme described in [17]. That is, given a committed value $c = \text{Commit}(b, r)$ for a given bit b , we recover b by solving a system of linear equations, therefore disproving the security claims made in [17].

Let us recall the problem we are attacking:

Problem 5. Given $c = (A, B, C) \star t_b$ with $t_b = \sum_{i=1}^{n-b} e_i \otimes e_i \otimes e_i$, $b \in \{0, \dots, n-1\}$, $(A, B, C) \in G$ sampled randomly, and \star is as defined in Equation 1, recover b .

Note, this problem is slightly more general than the commitment scheme from [17], since we are considering any $b \in \{0, 1, \dots, n-1\}$. From Problem 5, we see that c is precisely the tensor t_b with an isomorphism acting on it, as described in Lemma 2.

Lemma 3. *Let $t_b = \sum_{i=1}^{n-b} e_i \otimes e_i \otimes e_i$ then t_b has exactly b rank 0 points (up to scalar multiplication on the points).*

Proof. Let us write t_b as an n list of $n \times n$ matrices, which we denote T_b^1, \dots, T_b^n . These matrices can be described in the following way :

$$(T_b^k)_{ij} = \begin{cases} 1 & \text{if } i = j = k \text{ and } k \leq n - b \\ 0 & \text{otherwise} \end{cases}$$

We know that the rank of a point $u \in \mathbb{F}_q^n$ of t_b is the rank of the matrix $U_b = u_1 T_b^1 + \dots + u_n T_b^n$.

Using the above definition of the T_b^i , $i = 1, \dots, n$ we observe that U_b will be a diagonal matrix with entries

$$(U_b)_{ii} = \begin{cases} u_i, & \text{for } i = 1, \dots, n - b \\ 0 & \text{otherwise} \end{cases} .$$

Recall that we enforce that $u \neq 0 \in \mathbb{F}_q^n$, hence U_0 will have rank at least 1 and therefore no rank 0 points. Similarly U_1 will have one empty column so rank at most $n - 1$ and will always have a rank 0 point (up to scalar multiplication), in the form $u_1 = \dots = u_{n-1} = 0$ and u_n any non-zero element of \mathbb{F}_q^n . The same reasoning can be extended to t_b and U_b for further values of b to deduce the result. \square

We focus for a moment on the case $b \in \{0, 1\}$. Using Lemma 3, we have that t_1 has exactly one rank 0 point, and that t_0 has no rank 0 points. Combining this with Lemma 2 shows that we can use the existence of a rank 0 point as a distinguisher on c . We can find the rank 0 points of c by solving the system of n^2 linear equations

$$\alpha_1 G_1 + \dots + \alpha_n G_n = 0, \tag{3}$$

for $\alpha_i \in \mathbb{F}_q$, $i = 1, \dots, n$. If such a solution exists, then $b = 1$, else $b = 0$. For the more general case of $b \in \{0, 1, \dots, n - 1\}$, the number of distinct solutions will be exactly b .

While more complex algorithms could be used to solve this system, Gaussian elimination is sufficient for our purposes. The challenge here is selecting a set of n linearly independent equations from the n^2 possible choices. In the worst case this gives an upper bound on the number of operations of $O(n^4)$. Through experiments, however, we found that sampling the first n equations was sufficient for correctly solving the system. While we would not expect this to be true for a random set of n^2 equations, this could be due to the structure of the tensor which is not random. So heuristically, we expect a complexity of $O(n^3)$. This proves Theorem 1.

Theorem 1. *There exists an algorithm that solves Problem 5 using $O(n^4)$ operations.*

For all parameters highlighted in Section 2.4 the attack runs in under a second on a laptop.

Note that Theorem 1 always returns a correct answer to Problem 5. If we are satisfied with a probabilistic algorithm, then we can solve it in $O(n^3)$ operations using a different approach.

Theorem 2. *There exists a probabilistic algorithm that solves Problem 5 using $O(n^3)$ operations.*

Proof. We begin by restricting to the case $b \in \{0, 1\}$. Consider a random point $u \in \mathbb{F}_q^n$. Then u has rank n in t_0 and rank $n - 1$ in t_1 with very high probability.

Namely u will have rank n in t_0 with probability $(q-1)^n/q^n$ since there can be no zeros in this point. Similarly, in t_1 , one of the entries can be free but the rest must be non-zero, so we get probability $(q-1)^{n-1}/q^{n-1}$. By Lemma 2, these probabilities will translate to c . Thus, it suffices to compute the rank of u in the commitment, c , to recover b with overwhelming probability, for large q . This approach generalizes to $b \in \{0, 1, \dots, n-1\}$, in the obvious way.

This algorithm consists of computing a linear combination of n square matrices, and computing the sum's rank over the finite field \mathbb{F}_q . Using Gaussian elimination, we can do this in $O(n^3)$ complexity. \square

Remark 2. This attack method works because of how structured t_b is. For a random tensor we do not expect to have any rank 0 points (this will be shown in Lemmas 8 and 9). For this reason, our distinguishing attack is not expected to have any impact on the general case of Problem 2 (the Decisional Tensor Isomorphism Problem), which asks an attacker to determine whether two given tensors are isomorphic. For the same reason, we also do not claim any improvement on Problem 3 (the Computational Tensor Isomorphism Problem). To date, both of these problems are believed to be cryptographically hard in the general setting.

3.3 Stabilizer subgroup of t_b

We now investigate some elements belonging to the stabilizer group of tensors, and construct the entire stabilizer group of t_0 . These findings will be of use to us in an attack in later sections.

Stabilizers for all tensors. Recall, we define $v \in \mathbf{V}$ as

$$v := \sum_{i,j,k=1}^n v(i,j,k)e_i \otimes e_j \otimes e_k,$$

and we are considering isomorphisms $(A, B, C) \in G$ that act on v via the group action, (\star) , from Equation 1.

Lemma 4. *Let $\lambda_a, \lambda_b, \lambda_c \in \mathbb{F}_q$ be such that $\lambda_a \lambda_b \lambda_c = 1$. Then for all $v \in \mathbf{V}$, we have that $(\lambda_a I_n, \lambda_b I_n, \lambda_c I_n) \star v = v$.*

The proof of this lemma can be done straightforwardly using the definition of the group action from Equation 1. We reserve the details for Appendix A.

Stabilizer subgroup of t_b . Now we focus our attention to t_b , which can be written as

$$t_b := \sum_{i=1}^{n-b} e_i \otimes e_i \otimes e_i.$$

In the following two lemmas we formalize how diagonal matrices and permutation matrices can be used to create stabilizing elements for t_b , and more specifically, for t_0 .

Lemma 5. *Suppose $\Lambda_A, \Lambda_B, \Lambda_C$ are three diagonal $n \times n$ matrices over \mathbb{F}_q such that $\Lambda_A \Lambda_B \Lambda_C = I_n$. Then $(\Lambda_A, \Lambda_B, \Lambda_C) \star t_b = t_b$, i.e. $(\Lambda_A, \Lambda_B, \Lambda_C)$ is in the stabilizer subgroup of t_b .*

Proof. We claim that $(\Lambda_A, \Lambda_B, \Lambda_C)$ is an element of the stabilizing group of t_b . We can see this explicitly as

$$\begin{aligned} (\Lambda_A, \Lambda_B, \Lambda_C) \star t_b &= \sum_{i,j,k=1}^{n-b} \sum_{s=1}^{n-b} \Lambda_{is}^A \Lambda_{js}^B \Lambda_{ks}^C e_i \otimes e_j \otimes e_k \\ &= \sum_{i=1}^{n-b} \Lambda_{ii}^A \Lambda_{ii}^B \Lambda_{ii}^C e_i \otimes e_i \otimes e_i \text{ (the matrices are diagonal)} \\ &= \sum_{i=1}^{n-b} e_i \otimes e_i \otimes e_i = t_b. \end{aligned}$$

□

To explore how permutation matrices can be used to build stabilizing elements, we first focus on the case of $b = 0$. In what follows, we use S_n to denote the symmetric group of integers $\{1, \dots, n\}$.

Lemma 6. *Let $\sigma \in S_n$, and let P_σ be the associated permutation matrix given by $P_\sigma = (p_{ij})_{i,j=1}^n$ and $p_{ij} = \mathbf{1}_{i=\sigma(j)}$. Then $(P_\sigma, P_\sigma, P_\sigma) \star t_0 = t_0$, i.e. $(P_\sigma, P_\sigma, P_\sigma)$ is in the stabilizer subgroup of t_0 .*

Proof. Consider any permutation matrix P_σ . When applied consistently to the bases being used to construct $t_0 = \sum_{s=1}^n e_s \otimes e_s \otimes e_s$, it simply permutes the order in which the summation is performed, resulting in the same tensor t_0 . We reserve the explicit calculations showing this equality for Appendix A. □

In [10], Proposition 4.1, they state that the entire stabilizer group of t_b , defined over the complex numbers, is exactly the semi-direct product of the diagonal matrices from Lemma 5 and the set of permutation matrices P_σ for $\sigma \in S_{n-b}$. This is consistent with our findings over finite fields, and was further corroborated via our experiments.

Equivalence classes on G . The study of stabilizer groups leads us to a new equivalence definition on $G = \text{GL}(n, q) \times \text{GL}(n, q) \times \text{GL}(n, q)$. These observations will allow us to add more constraints to the solutions we are looking for in CTI, and thus accelerate our attack in the proceeding section.

Definition 12. *Let $(A_1, B_1, C_1), (A_2, B_2, C_2)$ be two elements from G , and $t \in \mathbf{V}$ a tensor. We say that (A_1, B_1, C_1) and (A_2, B_2, C_2) belong to the same equivalence class via t , denoted $(A_1, B_1, C_1) \equiv_t (A_2, B_2, C_2)$, if and only if they are equal up to pre-composition by an element in the stabilizer subgroup of t .*

3.4 Solving CTI in orbits of t_0

We focus on the $b = 0$ case from the commitment scheme, and outline an approach to recovering an element from the isomorphism class via t_0 of the secret (A, B, C) . Recall our problem is as follows:

Problem 6. Let $t_0, g \in \mathbf{V}$ be two 3-tensors such that

$$t_0 := \sum_{i=1}^n e_i \otimes e_i \otimes e_i, \text{ and } g := \sum_{i,j,k=1}^n g_{i,j,k} e_i \otimes e_j \otimes e_k$$

for $\{g_{i,j,k}\} \subset \mathbb{F}_q$. Assuming it exists, find an isomorphism $(A, B, C) \in G$ such that

$$(A, B, C) \star t_0 = g, \tag{4}$$

where \star is as defined in Equation 1.

The tensor t_0 has exactly n rank 1 points (up to scalars), so from Lemma 2 this tells us that g will also have n rank 1 points. Denote a set of rank 1 points of t_0 as $\{e_1, \dots, e_n\}$. Suppose we could find the rank 1 points in g , denoted $\{a_1, \dots, a_n\}$. Then, we can try to match the e_i to the a_i to recover part of the isomorphism, namely A^{-1} . We formalize this idea in Lemma 7.

Lemma 7. *Consider Problem 6.*

Let $\{a_1, \dots, a_n\}$ be the set of rank 1 points of g , and $\{e_1, \dots, e_n\}$ be the set of rank 1 points in t_0 (up to scalar multiplication). Then there exists an ordering of $\{a_1, \dots, a_n\}$ and a matrix A such that for each $i \in [1, \dots, n]$, $a_i = e_i A^{-1}$.

Proof. Recall that in any given tensor, we use three bases of \mathbb{F}_q^n to construct it. Each of these three bases plays a role in the expansion of the tensor. In the case of t_0 , we are using three copies of the canonical basis, $\{e_i\}_{i=1}^n$. The matrix A is acting as a change of basis map on one of these bases. Since A is invertible, we know the new basis, $\{Ae_i\}_{i=1}^n$, will also be a basis of \mathbb{F}_q^n .

This particular basis is what creates the list of matrices, and so plays an important role in how the linear combinations of these matrices interact. So as a consequence, this basis will house the smallest rank points of the tensor. For tensors of rank n , who have no rank 0 points, this will be all the rank 1 points. \square

Finding the rank 1 points $\{a_1, \dots, a_n\}$ is an instance of MinRank, so we can use the algorithm given in [4] that is summarized in Section 2.5. In this particular context, we want to find n matrices with target rank 1. This means that our coefficient variable matrix, R , is simply a row matrix. Denote the entries in R as r_1, \dots, r_n . This leaves us with a bilinear system in the target variables, $\{x_i\}_{i=1}^n$, and the coefficient variables, $\{r_i\}_{i=1}^n$, where we will have $n^2(n-1)/2$ equations and $n(n-1)$ monomials. From here we can solve by direct linearization. This fact, which we tested experimentally, corroborates the claims in [4] about the linear independence of these equations.

Going forward, Lemma 7 shows that we can recover some matrix A_0^{-1} whose rows are given by $\{a_i\}_{i=1}^n$. Our findings from Section 3.3 tell us that neither the permutation of these rows, nor the scalar multiples of them, will affect our search for a suitable isomorphism satisfying Equation 4. In fact, fixing these rows and scalar multiples is a good idea as it reduces the number of solutions and variables in our search.

Once we have recovered some A_0^{-1} , we can then solve for B_0 and C_0 to complete the isomorphism by considering the system of n^3 linear equations in $2n^2$ variables given by $(I, B_0, I) \star t_0 = (A_0^{-1}, I, C_0^{-1}) \star g$. The system, as is, is very under-determined because of the size of the equivalence class of (A, B, C) via t_0 , so to slim down the solution space, thanks to Lemma 5, we can similarly normalize $n - 1$ entries of the first row of B_0 by setting them to an arbitrary value of \mathbb{F}_q^* . Note that normalizing the n^{th} entry would increase our chance of failure too much, so we only normalize $n - 1$ of them.

There is a chance that this will not give a solution, in case two or more of the entries in the first row of B were necessarily 0. We argue in the proof of Theorem 3 that when q is much bigger than n , the probability of this failure is very low. In the small chance of failure, however, we can apply a new known isomorphism, $(A_1, B_1, C_1) \in G$, and now consider $(A_1, B_1, C_1) \star ((A, B, C) \star t_0) = (A_1, B_1, C_1) \star g$ instead. This essentially “rerandomizes” our instance, in the hopes that the solution space for $B_1 \cdot B$ will contain an entry with at most one column vector having a leading 0.

The above approach leaves us with $q - 1$ solutions, of which only one is not invertible. Hence, to further reduce the solution set we can normalize one additional entry in C_0^{-1} . Since we have already heavily restricted the first row of B_0 , this puts tight constraints on the first column of C_0^{-1} in the solution. Thus, the entry in C_0^{-1} we normalize must lie in a different column. This relationship between the rows of B_0 and the columns of C_0 can be seen when you consider the commitment, g , as a list of n matrices. For $g = [G_1, \dots, G_n]$, we have that

$$G_k = \begin{pmatrix} \sum_{s=1}^n A_{ks} B_{1s} C_{1s} & \dots & \sum_{s=1}^n A_{ks} B_{1s} C_{ns} \\ \vdots & \ddots & \vdots \\ \sum_{s=1}^n A_{ks} B_{ns} C_{1s} & \dots & \sum_{s=1}^n A_{ks} B_{ns} C_{ns} \end{pmatrix},$$

for $k \in [1, \dots, n]$.

Again, there is a $1/q$ probability of having no solution when this entry of C_0 is necessarily 0, but we can either use the previous approach of applying a known isomorphism, or simply run the same attack again, fixing a different entry of C_0 . After solving this system of equations, we are left with one solution. These steps are summarized in Figure 4.

Theorem 3. *There exists a probabilistic algorithm that solves Problem 6 using $O(n^6)$ operations.*

Proof. We first show that the probability of failure of Algorithm 4 is negligible for large q . When q is small, in case of failure one can just apply a new isomor-

- 1: **Given:** $g \in \mathbf{V}$, isomorphic to t_0 .
- 2: $a_1, \dots, a_n \leftarrow \text{MinRank}(g, \text{target rank} = 1)$
- 3: $A_0^{-1} \leftarrow \text{Matrix}(a_1, \dots, a_n)$
- 4: $B_0, C_0 \leftarrow \text{Solutions}((I, B_0, I) \star t_0 = (A_0^{-1}, I, C_0^{-1}) \star g) \cap \text{Solutions}((B_0)_{1,i} = 1, i = 1, \dots, n-1) \cap \text{Solutions}((C_0)_{n,n} = 1)$
- 5: **return** (A_0, B_0, C_0)

Fig. 4. Solving Problem 6.

phism $(A_1, B_1, C_1) \in G$ to g , and repeat the algorithm with this new instance as described above.

We have two independent chances of failure. The first occurs when we normalize the first $n-1$ entries of B_0 . Since we have already fixed A_0 , this fixes the permutation of columns of B_0 as well (see Lemma 6). Hence, we risk failure when one of these normalized columns necessarily has a leading zero. The chance of this happening is the complement probability to the first $n-1$ columns having no leading zero. We denote this event B_{fail} , and compute it to be

$$P(B_{fail}) = 1 - \frac{(q-1)^{n-1}}{q^{n-1}}.$$

The second chance of failure comes when we normalize an entry of C_0^{-1} . Similarly, there is a $1/q$ chance of failure here. This gives us a total probability of failure of

$$P(\text{Alg. 4 fails}) = P(B_{fail}) + \frac{1}{q},$$

which is negligible for large q .

We now prove the complexity of this algorithm. The dominating subroutines in Algorithm 4 include the MinRank computation, the tensor group action arithmetic, and solving the final system of equations (which can be done using Gaussian elimination). While the tensor arithmetic could be done in time $O(n^4)$, as noted in Section 6.2 of [42], the other two subroutines require $O(n^6)$ operations. \square

We test this attack on the parameters from Section 2.4 and give the results in seconds in Table 1. We consider some additional parameters in Figure 5 to further support our complexity claims.

n	q	time (s)
14	4093	9.3
22	4093	141.6
30	2039	858.9

Table 1. Timings in seconds for solving the CTI variant from Problem 6.

Timings for Algorithm 4

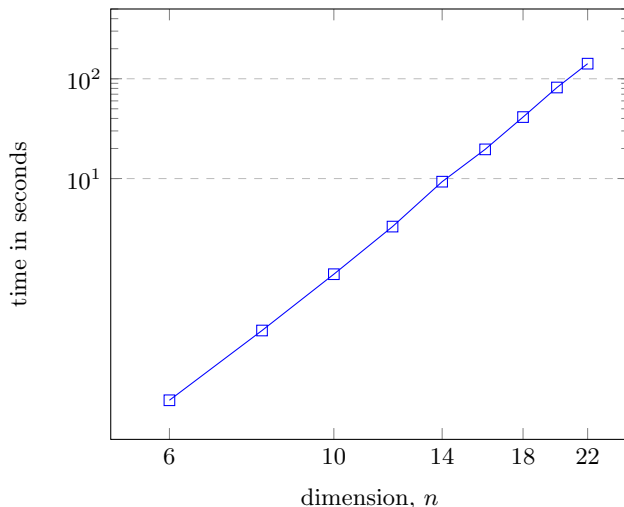


Fig. 5. We show some timings of Algorithm 4 for $q = 4093$ and varying values of n on a log-log scale. This corroborates our claim that Algorithm 4 has complexity $O(n^6)$, since the curve follows very closely to a line of slope 6.

Remark 3. In [17], they introduce an additional feature that their commitment scheme construction fulfills, called *linkability*. It essentially captures the idea that if two commitments are honestly generated, given some additional helper value called *linking material*, one can check whether they are committing to the same value. In fact, our attack on Problem 6 precisely allows to recompute the necessary linking material from the committed value only and break their *link secrecy* notion.

3.5 Solving CTI in orbits of t_1

The approach of computing the set of rank 1 points via the MinRank algorithm from [4] will only work in the case the tensor has rank n (i.e. $b = 0$ in the commitment scheme). Any smaller rank would result in too many rank 1 points to compute. In the $b = 1$ case, however, we can edit MinRank to further filter distinct rank 1 points using our knowledge of the stabilizer group of t_1 from Section 3.3.

We begin by computing the one rank 0 point in g (which is unique up to scalars). This point is easy to compute, as seen in Section 3.2. Denote it P_0 . Now, we know that any rank 1 point could have a rank 0 point added to it, and still remain a rank 1 point. In other words, we get an equivalency class on the set of rank 1 points where we say two rank 1 points, R_i, R_j , are equivalent if $R_i - R_j = \lambda P_0$ for some scalar λ . This means, for each $i \in [1, \dots, n - 1]$,

the equivalency class can be written as the subspace $\langle P_i, P_0 \rangle$, for some rank 1 point P_i , and the rank 0 point P_0 . Hence, we can obtain a representative from each equivalency class, P_i , by appropriately filtering the results returned from MinRank. To filter the solutions even more, we can normalize the first non-zero entry of the points.

After these computations, we will be left with one rank 0 point and $n - 1$ distinct rank 1 points. We are assured to get exactly $n - 1$ since each equivalency class, $\langle P_i, P_0 \rangle$, is the image under an isomorphism of the subspace $\langle e_i, e_n \rangle$. We can then carry out the rest of the attack described in Section 3.4, Figure 4, to reconstruct an isomorphism $(A_0, B_0, C_0) \equiv_{t_1} (A, B, C)$.

4 Repairing the Asiacrypt 2023 scheme

We propose a new construction in this section, and include proofs of its security. The key components that we aim to preserve from [17] are the following: a commitment scheme based on a non-transitive group action for which the group action should be uncertified (i.e. checking that two elements are in the same orbit is hard), and the commitment scheme should be non-interactive.

We therefore propose a non-interactive bit commitment scheme from non-transitive uncertified group actions, described in Figure 6. It is statistically binding (Theorem 4) and computationally hiding (Theorem 5). We improve on [28]’s construction, which is also statistically binding and computationally hiding but requires interaction. We lose the perfect binding of [17], however, this allows us to have a concrete instantiation that relies on standard problems. In practice, replacing perfect binding by statistical binding does not affect the security of more advanced constructions that could be built from bit commitments. Note that we do not keep the framework of Problem 5, but rather introduce a slightly different and simpler one, which still does not introduce any new assumptions.

Definition 13 (Decisional group action framework). *Consider a group action $\star : G \times V \rightarrow V$ that has the following properties :*

1. *It is an Effective Group Action.*
2. *Given two elements v_0, v_1 such that $v_1 = g \star v_0$ for some $g \in G$, computing g is hard.*
3. *The probability, p , that two random elements are in different orbits is $p = 1 - \text{negl}(\lambda)$.*
4. *The Decisional Group Action Inversion Problem for \star is hard (recall Definition 4).*

Note that the first three properties are described in [28].

Remark 4. One can extend the commitment scheme to accommodate a polynomial number of messages say $0, \dots, N$ by slightly modifying the Setup and Commit

<u>Setup(1^λ)</u>	<u>Commit(b)</u>	<u>Verify($b, (c, g)$)</u>
1: $v_0, v_1 \xleftarrow{\$} V$ 2: return v_0, v_1	1: $g \xleftarrow{\$} G$ 2: $c \leftarrow g \star v_b$ 3: return c	1: return $(c = g \star v_b)$

Fig. 6. Commitment scheme

algorithms of Figure 6. Indeed, during **Setup** one can instead randomly sample N elements v_0, \dots, v_N and output these. Then during **Commit**, to commit to a message $k \in \{0, \dots, N\}$, one samples $g \in G$ and computes $g \star v_k$.

Remark 5. Note that v_0, v_1 can be sampled as the output of a pseudo-random generator or a cryptographic hash function. What matters for our proofs is that they are indeed indistinguishable from a uniformly random distribution.

We can instantiate this framework using tensors through the group action described in Equation 1. The crucial difference with the construction of [17] is that v_0, v_1 are now two **randomly** generated tensors and they do not possess any special structure. In particular, a random tensor will only have low rank points with negligible probability, as shown in the following lemmas.

This means that our distinguishing attack from Section 3.2 is not applicable on a randomly generated instance.

Lemma 8. *The probability that a random tensor, $t \in \mathbf{V}$, has any rank r points is $p_r = \mathcal{O}(q^{(2r+1)n-n^2})$ for $r \ll n$.*

Though Lemma 8 is sufficient to support our claim that random tensors are not expected to have any low rank points, we leave its proof in Appendix A, and instead prove the following, stronger lemma.

Lemma 9. *Given a random tensor $t \in \mathbf{V}$, the average number of rank $n - d$ points (up to scalar multiplication) is q^{-d^2+n-1} as q goes to infinity.*

Proof. Consider our tensor t as a list of n random $n \times n$ matrices, over \mathbb{F}_q , say M_1, \dots, M_n . A rank r point in t is $\lambda = (\lambda_1, \dots, \lambda_n) \in \mathbb{F}_q^n$, $\lambda \neq 0$, such that $\text{rank}(\lambda_1 M_1 + \dots + \lambda_n M_n) = r$.

First, we have that the probability that a random matrix M has rank $n - d$ for some integer d goes to q^{-d^2} as q goes to infinity. This result is a direct observation from [22]. Then we observe that there are q^{n-1} possibilities projectively for λ , hence we get that the average number of rank $n - d$ points is q^{-d^2+n-1} . \square

Let us now check that all the desired properties from Definition 13 are satisfied : Property 1 has been studied in [28] and Property 2 corresponds to the Computational Tensor Isomorphism Problem (Problem 3). Property 4 is introduced in [17] and they discuss its applicability to tensors. While we show it is broken for their instantiation using structured tensors, t_b , it is still believed to be hard in the case of random tensors, which is precisely our case. Regarding

Property 3, we must compute the probability, p , of two random tensors being in different orbits under \star . Note that [28] assumes that this probability is high but they do not give any estimates.

Lemma 10. *The probability, p , of two random tensors being in distinct orbits under \star is $p \geq 1 - \frac{1}{q^{n^3-3n^2}}$.*

Proof. Let $t \in \mathbf{V}$ be a random tensor, then trivially

$$\#Orb(t) \leq \#G = (\#GL_n(q))^3 = O(q^{3n^2}).$$

Furthermore, we have $\#\mathbf{V} = q^{n^3}$. So the total number of orbits is at least $\#\mathbf{V}/(\#GL_n(q))^3 = O(q^{n^3-3n^2})$. The probability of two tensors being in the same orbit is therefore bounded by $\frac{1}{q^{n^3-3n^2}}$, hence $p \geq 1 - \frac{1}{q^{n^3-3n^2}}$. \square

We have shown that all the properties from Definition 13 are satisfied. Now it remains to show that our proposed commitment scheme from Figure 6 is both hiding and binding.

Theorem 4 (Binding). *The commitment scheme described in Figure 6 is statistically binding.*

Proof. Consider \mathbf{G} to be the binding security game applied to our scheme. Taking the following probabilities over the randomness of the game we have :

$$\begin{aligned} \Pr[\mathbf{G}(\mathcal{A}) \rightarrow 1] &= \Pr[\mathbf{G}(\mathcal{A}) \rightarrow 1 \wedge v_0, v_1 \text{ are in the same orbit}] \\ &\quad + \Pr[\mathbf{G}(\mathcal{A}) \rightarrow 1 \wedge v_0, v_1 \text{ are in different orbits}] \\ &\leq \Pr[v_0, v_1 \text{ are in the same orbit}] \\ &\quad + \Pr[\mathbf{G}(\mathcal{A}) \rightarrow 1 | v_0, v_1 \text{ are in different orbits}] \cdot p, \end{aligned}$$

where p is the probability defined by Property 3, and computed in Lemma 10. We have $\Pr[v_0, v_1 \text{ are in the same orbit}] = 1 - p$ by definition of p . Furthermore, $\Pr[\mathbf{G}(\mathcal{A}) \rightarrow 1 | v_0, v_1 \text{ are in different orbits}] = 0$ since otherwise if \mathcal{A} wins \mathbf{G} in that case, this means they return (A_0, B_0, C_0) and (A_1, B_1, C_1) such that

$$(A_0, B_0, C_0) \star v_0 = (A_1, B_1, C_1) \star v_1.$$

In particular this would mean that $(A_1^{-1}A_0, B_1^{-1}B_0, C_1^{-1}C_0) \star v_0 = v_1$ which is impossible since v_0, v_1 are in different orbits and thus so no such isomorphism exists.

Overall we get

$$\Pr[\mathbf{G}(\mathcal{A}) \rightarrow 1] \leq (1 - p) + 0 \cdot p = (1 - p) = \text{negl}(\lambda).$$

\square

Remark 6. Notice that in the case where v_0, v_1 are indeed in the same orbit (which happens only with negligible probability), breaking the Binding problem amounts to solving the Computational Tensor Isomorphism problem (Problem 3) in a *random* orbit, hence remains plausibly hard.

Theorem 5 (Hiding). *Assuming the hardness of the dGA-IP problem (Definition 4), our commitment scheme is hiding.*

Proof. Consider G to be the hiding game. Taking the following probabilities over the randomness of the game, we have :

$$\begin{aligned} \Pr[G(\mathcal{A}) \rightarrow 1] &= \Pr[G(\mathcal{A}) \rightarrow 1 \wedge v_0, v_1 \text{ are in the same orbit}] \\ &\quad + \Pr[G(\mathcal{A}) \rightarrow 1 \wedge v_0, v_1 \text{ are in different orbits}] \\ &\leq \Pr[v_0, v_1 \text{ are in the same orbit}] \\ &\quad + \Pr[G(\mathcal{A}) \rightarrow 1 | v_0, v_1 \text{ are in different orbits}] \cdot p, \end{aligned}$$

where p is the probability defined by Property 3. We have $\Pr[v_0, v_1 \text{ are in the same orbit}] = 1 - p = \text{negl}(\lambda)$.

In the case where v_0, v_1 are in different orbits, one can refer to [17], Theorem 2. Roughly, given an adversary \mathcal{B} against dGA-IP, that receives as input s, t , they instantiate two Hiding games with adversaries $\mathcal{A}_1, \mathcal{A}_2$ to which they respectively give s or t as input, and \mathcal{B} returns 1 if the outputs of \mathcal{A}_1 and \mathcal{A}_2 are equal and 0 otherwise. They get that

$$\Pr[G(\mathcal{A}) \rightarrow 1 | v_0, v_1 \text{ are in different orbits}] \leq \frac{1}{2} + 2\epsilon(\lambda)^2$$

where $\epsilon(\lambda)$ is the advantage in the dGA-IP game.

So overall we have

$$\begin{aligned} \Pr[G(\mathcal{A}) \rightarrow 1] &\leq (1 - p) + p \cdot \left(\frac{1}{2} + 2\epsilon(\lambda)^2\right) \\ &= \frac{1}{2}p + (1 - p) + 2p\epsilon(\lambda)^2 \end{aligned}$$

and by assumption both $\epsilon(\lambda)$ and $1 - p$ are negligible. \square

Remark 7. Consider the extension of our commitment scheme to a message space of $\{0, \dots, N\}$ as described in Remark 4. Then the hiding and binding properties are derived in a straightforward way since v_0, \dots, v_N are in different orbits with probability $1 - \frac{N}{q^{n^3 - 3n^2}}$.

4.1 On proofs of knowledge

To use commitment schemes within more advanced protocols such as verifiable secret sharing or zero-knowledge proofs for generic statements, it is useful to have non-interactive zero-knowledge proofs of knowledge of commitments. More precisely, one wishes to prove that they know the value to which a commitment c corresponds without giving away any information about it.

Let us consider the commitment scheme of Figure 6, extended to the message space $\{0, \dots, N\}$. Given public parameters $\mathbf{pp} = \{t_0, \dots, t_N\}$ consisting of $N + 1$ random tensors from \mathbf{V} , we consider the relation

$$\mathcal{R} = \{(c, (t_i, (A, B, C))) \mid c = (A, B, C) \star t_i\},$$

where c is the statement and $(t_i, (A, B, C))$ is the witness. This means given c we wish to prove knowledge of the message t_i and randomness (A, B, C) to which c corresponds, without revealing anything about it. We briefly expose two ways of obtaining such a proof.

Using OR-proofs. A proof for \mathcal{R} can be obtained by combining an OR-proof [16] and a proof for $\mathcal{R}_i = \{(c, t_i, (A, B, C)) \mid c = (A, B, C) \star t_i\}$, to show that one knows one out of the N t_i 's. A proof for \mathcal{R} can be obtained by adapting, for example, the graph isomorphism proof [23]. However, using OR-proofs increases the communication cost in the answer of the prover, and we will therefore prefer to build a direct proof for the full relation \mathcal{R} .

A direct proof for \mathcal{R} . We give in Figure 7 a sigma protocol that directly gives a proof for \mathcal{R} .

$\text{Prover}_1(\mathbf{pp}, t_i, c, (A, B, C))$ 1: $A', B', C' \xleftarrow{\$} \text{GL}_n(q)^3$ 2: $\sigma \xleftarrow{\$} S_n$ 3: for $j = 1, \dots, N$ do 4: $d_j \leftarrow (A', B', C') \star t_{\sigma(j)}$ 5: end for 6: $st \leftarrow (\mathbf{pp}, (A, B, C), (A', B', C'), \sigma)$ 7: Send $(d_j)_{j=1}^N$ to Verifier 8: return st	$\text{Verifier}_1(\mathbf{pp}, c, (d_j)_{j=1}^N)$ 1: $ch \xleftarrow{\$} \{0, 1\}$ 2: $st \leftarrow (\mathbf{pp}, ch, c, (d_j)_{j=1}^N, t_i)$ 3: Send ch to Prover 4: return st
$\text{Prover}_2(st, ch)$ 1: if $ch = 0$ then 2: $resp \leftarrow ((A', B', C'), \sigma)$ 3: return $resp$ 4: end if 5: $resp \leftarrow (A(A')^{-1}, B(B')^{-1}, C(C')^{-1}, i)$ 6: return $resp$	$\text{Verifier}_2(st, resp)$ 1: if $ch = 0$ then 2: $resp \rightarrow ((\tilde{A}, \tilde{B}, \tilde{C}), \sigma)$ 3: return $\forall i, (\tilde{A}, \tilde{B}, \tilde{C}) \star t_{\sigma(i)} = d_i$ 4: end if 5: $resp \rightarrow (\tilde{A}, \tilde{B}, \tilde{C}, i)$ 6: return $((\tilde{A}, \tilde{B}, \tilde{C}) \star d_i = c)$

Fig. 7. Proof system for \mathcal{R}

We sketch the extractor for special soundness and simulator for honest-verifier zero-knowledge below.

Special-soundness. Suppose we have two accepting transcripts with different challenges, $((d_j)_{j=1}^N, \text{ch}_0, \text{resp}_0)$ and $((d_j)_{j=1}^N, \text{ch}_1, \text{resp}_1)$. Without loss of generality, we assume $\text{ch}_0 = 0$. Then we can build an extractor \mathcal{E} which, given these transcripts as input, does the following : Recover (A', B', C') from resp_0 and $(A(A')^{-1}, B(B')^{-1}, C(C')^{-1})$ from resp_1 . Compute (A, B, C) by multiplying the latter by the former. Recover i from resp_0 and recover the correct $t_{\sigma^{-1}(i)}$. Then $(t_{\sigma^{-1}(i)}, (A, B, C))$ is the witness.

Honest-verifier zero-knowledge. We now sketch the simulator. In the case $\text{ch} = 0$, the simulator just follows the protocol honestly and will be producing an accepting transcript. In the $\text{ch} = 1$ case, the simulator samples (A', B', C') and σ as in the protocol, then picks some index j and sets $d_j = ((A')^{-1}, (B')^{-1}, (C')^{-1}) \star c$. The other d_i for $i \neq j$ are computed according to the protocol. The distribution will remain the same since (A', B', C') is random. The answer then consists of j and (A', B', C') .

5 Conclusion

In this work, we study low rank points and stabilizers on structured tensors. We show how this information gives us the tools to break the hiding property of the bit commitment scheme proposed in [17] at Asiacrypt 2023, that uses these structured tensors. Our attacks further allow to recover all the secret information used during the creation of the commitment. All of these algorithms run in polynomial time, which leaves the framework introduced in [17] with no concrete instantiation. Prior to this work, there was no evidence in the literature suggesting that structured tensors were not secure for use in cryptography.

With these attacks in mind, we propose a slightly different framework as well as a construction that makes use of *random* tensors. This allows us to build a statistically binding, computationally hiding commitment from non-transitive group actions. Finally, we complete this work by proposing a zero-knowledge proof of opening for our new commitment scheme.

At the moment, the field of commitment schemes from non-transitive group actions is lacking protocols that are both post-quantum and non-interactive. We hope our new construction helps to fill this gap, and that our attacks can help to inform future cryptography designers on some of the limits of working with structured tensors. We leave any further investigation into a commitment scheme using the framework proposed in [17] as future work.

References

1. Alamati, N., Feo, L.D., Montgomery, H., Patranabis, S.: Cryptographic group actions and applications. *IACR Cryptol. ePrint Arch.* p. 1188 (2020), <https://eprint.iacr.org/2020/1188>
2. Albrecht, M.R., Fenzi, G., Lapiha, O., Nguyen, N.K.: SLAP: succinct lattice-based polynomial commitments from standard assumptions. *Cryptology ePrint Archive*, Paper 2023/1469 (2023), <https://eprint.iacr.org/2023/1469>
3. Aragon, N., Gaborit, P., Hauteville, A., Tillich, J.: A new algorithm for solving the rank syndrome decoding problem. In: 2018 IEEE International Symposium on Information Theory, ISIT 2018, Vail, CO, USA, June 17-22, 2018. pp. 2421–2425. IEEE (2018). <https://doi.org/10.1109/ISIT.2018.8437464>
4. Bardet, M., Bros, M., Cabarcas, D., Gaborit, P., Perlner, R.A., Smith-Tone, D., Tillich, J., Verbel, J.A.: Improvements of algebraic attacks for solving the rank decoding and MinRank problems. In: Moriai, S., Wang, H. (eds.) *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security*, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I. *Lecture Notes in Computer Science*, vol. 12491, pp. 507–536. Springer (2020). https://doi.org/10.1007/978-3-030-64837-4_17
5. Barengi, A., Biasse, J., Persichetti, E., Santini, P.: On the computational hardness of the code equivalence problem in cryptography. *Adv. Math. Commun.* **17**(1), 23–55 (2023). <https://doi.org/10.3934/AMC.2022064>
6. Baum, C., Damgård, I., Lyubashevsky, V., Oechsner, S., Peikert, C.: More efficient commitments from structured lattice assumptions. In: Catalano, D., De Prisco, R. (eds.) *Security and Cryptography for Networks*. pp. 368–385. Springer International Publishing, Cham (2018)
7. Beullens, W.: Not enough LESS: An improved algorithm for solving code equivalence problems over F_q . In: *International Conference on Selected Areas in Cryptography*. pp. 387–403. Springer (2020)
8. Bouillaguet, C., Fouque, P., Véber, A.: Graph-theoretic algorithms for the “isomorphism of polynomials” problem. In: Johansson, T., Nguyen, P.Q. (eds.) *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Athens, Greece, May 26-30, 2013. Proceedings. *Lecture Notes in Computer Science*, vol. 7881, pp. 211–227. Springer (2013). https://doi.org/10.1007/978-3-642-38348-9_13, https://doi.org/10.1007/978-3-642-38348-9_13
9. Brassard, G., Yung, M.: One-way group actions. In: *Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology*. p. 94–107. CRYPTO ’90, Springer-Verlag, Berlin, Heidelberg (1990)
10. Bürgisser, P., Ikenmeyer, C.: Geometric complexity theory and tensor rank. *CoRR* **abs/1011.1350** (2010), <http://arxiv.org/abs/1011.1350>
11. Chen, M., Lai, Y.F., Laval, A., Marco, L., Petit, C.: Malleable commitments from group actions and zero-knowledge proofs for circuits based on isogenies. *Cryptology ePrint Archive*, Paper 2023/1710 (2023), <https://eprint.iacr.org/2023/1710>
12. Chou, T., Niederhagen, R., Persichetti, E., Ran, L., Randrianarisoa, T.H., Reijnders, K., Samardjiska, S., Trimoska, M.: Matrix equivalence digital signature (2023), <https://www.meds-pqc.org/spec/MEDS-2023-07-26.pdf>
13. Chou, T., Niederhagen, R., Persichetti, E., Randrianarisoa, T.H., Reijnders, K., Samardjiska, S., Trimoska, M.: Take your MEDS: digital signatures from matrix code equivalence. In: Mrabet, N.E., Feo, L.D., Duquesne, S. (eds.) *Progress in*

- Cryptology - AFRICACRYPT 2023 - 14th International Conference on Cryptology in Africa, Sousse, Tunisia, July 19-21, 2023, Proceedings. Lecture Notes in Computer Science, vol. 14064, pp. 28–52. Springer (2023). https://doi.org/10.1007/978-3-031-37679-5_2
14. Couveignes, J.M.: Hard homogeneous spaces. Cryptology ePrint Archive, Paper 2006/291 (2006), <https://eprint.iacr.org/2006/291>
 15. Couvreur, A., Debris-Alazard, T., Gaborit, P.: On the hardness of code equivalence problems in rank metric. CoRR **abs/2011.04611** (2020), <https://arxiv.org/abs/2011.04611>
 16. Cramer, R., Damgård, I., Schoenmakers, B.: Proofs of partial knowledge and simplified design of witness hiding protocols. In: Desmedt, Y.G. (ed.) *Advances in Cryptology — CRYPTO '94*. pp. 174–187. Springer Berlin Heidelberg, Berlin, Heidelberg (1994)
 17. D’Alconzo, G., Flamini, A., Gangemi, A.: Non-interactive commitment from non-transitive group actions. *Advances in Cryptology – ASIACRYPT 2023* p. 723 (2023), <https://eprint.iacr.org/2023/723>
 18. Ducas, L., van Woerden, W.P.J.: On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In: Dunkelman, O., Dziembowski, S. (eds.) *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*. Lecture Notes in Computer Science, vol. 13277, pp. 643–673. Springer (2022). https://doi.org/10.1007/978-3-031-07082-2_23
 19. Fenzi, G., Moghaddas, H., Nguyen, N.K.: Lattice-based polynomial commitments: Towards asymptotic and concrete efficiency. Cryptology ePrint Archive, Paper 2023/846 (2023), <https://eprint.iacr.org/2023/846>
 20. Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. vol. 263 (03 1999). https://doi.org/10.1007/3-540-47721-7_12
 21. Frederiksen, T.K., Pinkas, B., Yanai, A.: Committed MPC - maliciously secure multiparty computation from homomorphic commitments. In: Abdalla, M., Dahab, R. (eds.) *Public-Key Cryptography - PKC 2018 - 21st IACR International Conference on Practice and Theory of Public-Key Cryptography, Rio de Janeiro, Brazil, March 25-29, 2018, Proceedings, Part I*. Lecture Notes in Computer Science, vol. 10769, pp. 587–619. Springer (2018). https://doi.org/10.1007/978-3-319-76578-5_20
 22. Fulman, J., Goldstein, L.: Stein’s method and the rank distribution of random matrices over finite fields. *The Annals of Probability* **43**(3) (May 2015). <https://doi.org/10.1214/13-aop889>
 23. Goldreich, O., Micali, S., Wigderson, A.: Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *J. ACM* **38**(3), 690–728 (jul 1991). <https://doi.org/10.1145/116825.116852>
 24. Grochow, J.A., Qiao, Y.: Isomorphism problems for tensors, groups, and cubic forms: completeness and reductions. CoRR **abs/1907.00309** (2019), <http://arxiv.org/abs/1907.00309>
 25. Håstad, J.: Tensor rank is NP-complete. *J. Algorithms* **11**(4), 644–654 (1990). [https://doi.org/10.1016/0196-6774\(90\)90014-6](https://doi.org/10.1016/0196-6774(90)90014-6)
 26. Hillar, C.J., Lim, L.: Most tensor problems are NP-hard. *J. ACM* **60**(6), 45:1–45:39 (2013). <https://doi.org/10.1145/2512329>
 27. Jain, A., Krenn, S., Pietrzak, K., Tentes, A.: Commitments and efficient zero-knowledge proofs from learning parity with noise. In: Wang, X., Sako, K. (eds.)

- Advances in Cryptology – ASIACRYPT 2012. pp. 663–680. Springer Berlin Heidelberg, Berlin, Heidelberg (2012)
28. Ji, Z., Qiao, Y., Song, F., Yun, A.: General linear group action on tensors: A candidate for post-quantum cryptography. In: Hofheinz, D., Rosen, A. (eds.) Theory of Cryptography - 17th International Conference, TCC 2019, Nuremberg, Germany, December 1-5, 2019, Proceedings, Part I. Lecture Notes in Computer Science, vol. 11891, pp. 251–281. Springer (2019). https://doi.org/10.1007/978-3-030-36030-6_11
 29. Juels, A., Luby, M., Ostrovsky, R.: Security of blind digital signatures (extended abstract). In: Jr., B.S.K. (ed.) Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings. Lecture Notes in Computer Science, vol. 1294, pp. 150–164. Springer (1997). <https://doi.org/10.1007/BFB0052233>
 30. Leon, J.: Computing automorphism groups of error-correcting codes. IEEE Transactions on Information Theory **28**(3), 496–511 (1982)
 31. Lyubashevsky, V., Nguyen, N.K., Seiler, G.: Shorter lattice-based zero-knowledge proofs via one-time commitments. In: Garay, J.A. (ed.) Public-Key Cryptography - PKC 2021 - 24th IACR International Conference on Practice and Theory of Public Key Cryptography, Virtual Event, May 10-13, 2021, Proceedings, Part I. Lecture Notes in Computer Science, vol. 12710, pp. 215–241. Springer (2021). https://doi.org/10.1007/978-3-030-75245-3_9
 32. Morozov, K., Roy, P.S., Sakurai, K.: On unconditionally binding code-based commitment schemes. In: Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication. IMCOM '17, Association for Computing Machinery, New York, NY, USA (2017). <https://doi.org/10.1145/3022227.3022327>, <https://doi.org/10.1145/3022227.3022327>
 33. Naor, M.: Bit commitment using pseudorandomness. J. Cryptol. **4**(2), 151–158 (1991). <https://doi.org/10.1007/BF00196774>
 34. Ostrovsky, R., Persiano, G., Visconti, I.: Simulation-based concurrent non-malleable commitments and decommitments. In: Reingold, O. (ed.) Theory of Cryptography, 6th Theory of Cryptography Conference, TCC 2009, San Francisco, CA, USA, March 15-17, 2009. Proceedings. Lecture Notes in Computer Science, vol. 5444, pp. 91–108. Springer (2009). https://doi.org/10.1007/978-3-642-00457-5_7
 35. Patarin, J.: Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In: Maurer, U.M. (ed.) Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding. Lecture Notes in Computer Science, vol. 1070, pp. 33–48. Springer (1996). https://doi.org/10.1007/3-540-68339-9_4
 36. Pedersen, T.P.: Non-interactive and information-theoretic secure verifiable secret sharing. In: Feigenbaum, J. (ed.) Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings. Lecture Notes in Computer Science, vol. 576, pp. 129–140. Springer (1991). https://doi.org/10.1007/3-540-46766-1_9
 37. Poelstra, A., Back, A., Friedenbach, M., Maxwell, G., Wuille, P.: Confidential assets. In: Zohar, A., Eyal, I., Teague, V., Clark, J., Bracciali, A., Pintore, F., Sala, M. (eds.) Financial Cryptography and Data Security - FC 2018 International Workshops, BITCOIN, VOTING, and WTSC, Nieuwpoort, Curaçao, March 2, 2018,

- Revised Selected Papers. Lecture Notes in Computer Science, vol. 10958, pp. 43–63. Springer (2018). https://doi.org/10.1007/978-3-662-58820-8_4
38. Reijnders, K., Samardjiska, S., Trimoska, M.: Hardness estimates of the code equivalence problem in the rank metric. IACR Cryptol. ePrint Arch. p. 276 (2022), <https://eprint.iacr.org/2022/276>
 39. Rostovtsev, A., Stolbunov, A.: Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Paper 2006/145 (2006), <https://eprint.iacr.org/2006/145>
 40. Schaefer, M., Stefankovic, D.: The complexity of tensor rank. Theory Comput. Syst. **62**(5), 1161–1174 (2018). <https://doi.org/10.1007/S00224-017-9800-Y>
 41. Sterner, B.: Commitment schemes from supersingular elliptic curve isogeny graphs. Cryptology ePrint Archive, Paper 2021/1031 (2021), <https://eprint.iacr.org/2021/1031>
 42. Tang, G., Duong, D.H., Joux, A., Plantard, T., Qiao, Y., Susilo, W.: Practical post-quantum signature schemes from isomorphism problems of trilinear forms. In: Dunkelman, O., Dziembowski, S. (eds.) Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III. Lecture Notes in Computer Science, vol. 13277, pp. 582–612. Springer (2022). https://doi.org/10.1007/978-3-031-07082-2_21

Supplementary Material

A Proofs

All of the proofs included here are done via a very computational approach, using core definitions. We encourage the reader who wants to familiarize themselves with these definitions to do them as exercise.

Lemma 4. Let $\lambda_a, \lambda_b, \lambda_c \in \mathbb{F}_q$ be such that $\lambda_a \lambda_b \lambda_c = 1$. Then for all $v \in \mathbf{V}$, we have that $(\lambda_a I_n, \lambda_b I_n, \lambda_c I_n) \star v = v$.

Proof. Let us write $v = \sum_{i,j,k=1}^n v(i,j,k) e_i \otimes e_j \otimes e_k$. We have

$$\begin{aligned}
 (\lambda_a I_n, \lambda_b I_n, \lambda_c I_n) \star v &= \sum_{i,j,k=1}^n v(i,j,k) (\lambda_a I_n) e_i \otimes (\lambda_b I_n) e_j \otimes (\lambda_c I_n) e_k \\
 &= \sum_{i,j,k=1}^n v(i,j,k) \lambda_a \lambda_b \lambda_c e_i \otimes e_j \otimes e_k \\
 &= \sum_{i,j,k=1}^n v(i,j,k) e_i \otimes e_j \otimes e_k \text{ since } \lambda_a \lambda_b \lambda_c = 1 \\
 &= v
 \end{aligned}$$

Lemma 6. Let $\sigma \in S_n$, then there exists P_σ such that $(P_\sigma, P_\sigma, P_\sigma) \star t_0 = t_0$, given by $P_\sigma = (p_{ij})_{i,j=1}^n$ and $p_{ij} = \mathbf{1}_{i=\sigma(j)}$.

Proof. Let $t_0 = \sum_{s=1}^n e_s \otimes e_s \otimes e_s$, then we can express the action $(A, B, C) \star t_0$ (from 1) as $(A, B, C) * (\sum_{s=1}^n e_s \times e_s \times e_s) = \sum_{i,j,k} \sum_{s=1}^n A_{is} B_{js} C_{ks} e_i \times e_j \times e_k$.

$$\begin{aligned}
 (P_\sigma, P_\sigma, P_\sigma) \star t_0 &= \sum_{i,j,k=1}^n \sum_{s=1}^n (P_\sigma)_{is} (P_\sigma)_{js} (P_\sigma)_{ks} e_i \otimes e_j \otimes e_k \\
 &= \sum_{i,j,k=1}^n \sum_{s=1}^n \mathbf{1}_{i=\sigma(s)} \mathbf{1}_{j=\sigma(s)} \mathbf{1}_{k=\sigma(s)} e_i \otimes e_j \otimes e_k \\
 &= \sum_{i,j,k=1}^n \sum_{s=1}^n \mathbf{1}_{i=j=k} \mathbf{1}_{i=\sigma(s)} e_i \otimes e_j \otimes e_k \\
 &= \sum_{m=1}^n \sum_{s=1}^n \mathbf{1}_{m=\sigma(s)} e_m \otimes e_m \otimes e_m \\
 &= \sum_{m=1}^n e_m \otimes e_m \otimes e_m = t_0
 \end{aligned}$$

since σ is a bijection.

Lemma 8. The probability that a random 3-tensor, $t \in \mathbf{V}$, has any rank r points is $p_r = \mathcal{O}(q^{(2r+1)n-n^2})$ for $r \ll n$.

Proof. Consider our tensor t as a list of n random $n \times n$ matrices, over \mathbb{F}_q , say M_1, \dots, M_n .

For t to have a rank r point, means there exists $\lambda = (\lambda_1, \dots, \lambda_n) \in \mathbb{F}_q^n$, $\lambda \neq 0$, such that $\text{rank}(\lambda_1 M_1 + \dots + \lambda_n M_n) = r$.

We begin by proving:

- (1) given a random matrix M , we will start by estimating the probability that it is in the span of M_1, \dots, M_n ;
- (2) then we will compute the number of matrices of a given rank.

Finally, we will combine these results together to evaluate the probability that $U = \lambda_1 M_1 + \dots + \lambda_n M_n$ has rank r .

Let us start with (1). Given a random matrix M we want to estimate the probability p_1 that M belongs to the linear span of M_1, \dots, M_n . If M is the zero matrix then $p_1 = 1$ but this only happens with probability $1/q^{n^2}$. Let k be the dimension of the linear span, then

$$p_1 = \sum_{k=1}^n \frac{q^k}{q^{n^2}} \cdot \Pr[\text{linear span has dimension } k].$$

For large n, q , we get that the span has dimension n with high probability, namely

$$\Pr[\text{linear span has dimension } n] = \frac{q^{n^2} - 1}{q^{n^2}} \frac{q^{n^2} - q}{q^{n^2}} \frac{q^{n^2} - q^2}{q^{n^2}} \dots \frac{q^{n^2} - q^{n-1}}{q^{n^2}} \approx 1.$$

Hence we get $p_1 = \mathcal{O}(q^{n-n^2})$.

Let us now move on to (2). We are interested in low rank points since these are the easiest to compute, hence we assume $r \ll n$. To compute the number of matrices of rank r , let us consider a decomposition of the form $M = SR$ as in Section 2.5. S is an $n \times r$ matrix of rank r which consists of the row space of M , and R is an $r \times n$ matrix of rank r corresponding to the column space of M . Note that this decomposition is not unique since for any $r \times r$ invertible matrix Q , SQ and $Q^{-1}R$ is also a valid decomposition for M . In other words $SQQ^{-1}R = M$. To estimate the number of rank r matrices we thus estimate the number of possibilities for S, R and Q . For S and R , given $r \ll n$, the number of possible choices for a space of dimension r is $N_1 = (q^n - 1) \cdot (q^n - q) \dots (q^n - q^{r-1}) = \mathcal{O}(q^{nr})$. For an invertible $r \times r$ matrix, the number of possible choices is $N_2 = \mathcal{O}(q^{r^2})$. Hence the total number of rank r matrices is given by $N_1^2/N_2 = \mathcal{O}(\frac{q^{2nr}}{q^{r^2}}) = \mathcal{O}(q^{2nr})$. So in conclusion the probability that $M = \lambda_1 M_1 + \dots + \lambda_n M_n$ has rank r , $r \ll n$, is given by

$$p_r = p_1 \cdot \frac{N_1^2}{N_2} = \mathcal{O}(q^{n-n^2} \cdot q^{2nr}) = \mathcal{O}(q^{(2r+1)n-n^2}).$$

□